VZCZCXYZ0000
RR RUEHWEB

DE RUEHMN #0947/01 3051600
ZNY CCCCC ZZH
R 011600Z NOV 07
FM AMEMBASSY MONTEVIDEO
TO RUEHC/SECSTATE WASHDC 7705
INFO RUCNMER/MERCOSUR COLLECTIVE
RUMIAAA/CDR USSOUTHCOM MIAMI FL
RUEHC/SECSTATE WASHDC 7706
RUCNFB/FBI WASHDC
RUEAHLC/HOMELAND SECURITY CENTER WASHINGTON DC
RUEAIIA/CIA WASHDC

CONFIDENTIAL MONTEVIDEO 000947

SIPDIS

SIPDIS

STATE FOR S/CT KEN MCKUNE
CIA FOR NCTC
BUENOS AIRES FOR LEGATT (WGODOY) AND DHS/ICE (DFREEMAN)
SOUTHCOM FOR POLAD

E.O. 12958: DECL: 10/31/2017
TAGS: PTER KVPR PREL PGOV PINR CVIS ASEC KHLS PBTS
UY
SUBJECT: URUGUAY ON HOST GOVERNMENT PRACTICES - INFORMATION
COLLECTION, SCREENING AND SHARING

REF: STATE 133921

Classified By: CHARGE D'AFFAIRES PETER X. HARDING
FOR REASONS 1.4 (b) and (d).

¶1. (C) Introduction: This telegram responds to reftel action request for information. Methodology and sources used to compile this report included an in-depth interview by regional LEGATT (Buenos Aires) with Dra. Carmen Conte, Director, Direccion Nacional de Migracion and with Comisario Jorge Scelza Stiya, Director de Migraciones at Aeropuerto Internacional de Carrasco on October 4, 2007. Additional information was provided by the Embassy's RSO, Political and Consular sections, other agencies at post and contacts. End Introduction.

¶2. (C) Begin report.

¶A. Watchlisting

-- Q. If host government maintains a "watchlist," how many records does the watchlist contain, and how many are terrorist-related?
-- A. The Direccion Nacional de Migracion (DNM) maintains a computerized database with the names of INTERPOL fugitives, Uruguayan fugitives, minors with travel restrictions, and persons with civil and/or criminal travel restrictions. None are terrorist-related.

-- Q. Which ministry or office maintains the watchlist?
-- A. The Direccion Nacional de Migracin (DNM), Ministry of Interior

----
¶B. Traveler Information Collection

-- Q. What are the country's policies (legislation, mandates, etc.) on collecting information from travelers arriving in the country?
-- A. The DNM is only authorized to collect very basic information regarding travelers and is not allowed to request additional information. Collected information includes; travel document (passport) information, mode and purpose of

travel, and destination.

-- Q. Are there different policies for air, sea, and land entry and for domestic flights?
-- A. No, they are same for all.

-- Q. Who collects traveler information?
-- A. Direccion Nacional de Migracion (DNM). Customs also collects information on transfers of money over $10,000.00

-- Q. What are the policies of the collecting agency to share that information with foreign governments?
-- A. There are no formal policies, but DNM cooperates with requests for information from other countries. The consular section has received excellent cooperation in efforts to locate American citizens (AMCITs) for welfare and whereabouts inquiries, as well as verifying travel for Non-Immigrant Visa (NIV) purposes.

-- Q. Does the host government collect Passenger Name Record (PNR) data on incoming commercial flights or vessels? Is this data used for intelligence or law enforcement purposes to screen travelers? Does host government have any existing treaties to share PNR data?
-- A. Yes on the first question. No on the other two questions.

-- Q. If applicable, have advance passenger information systems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals?
-- A. Not applicable. DNM is not authorized to receive passenger lists from the airlines.

¶C. Border Control and Screening

-- Q. Does the host government employ software to screen travelers of security interest?
-- A. No.

-- Q. Are all travelers tracked electronically, or only non-host-country nationals? What is the frequency of travelers being "waived through" because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically? What is the estimated percentage of non-recorded crossings, entries and exits?
-- A. Entry and departure at major ports of entry is tracked electronically. DNM provides travel history for NIV applicants at the applicant's request. At land borders crossings with Argentina and Brazil, inspection of vehicles and identify documents is sporadic at best and at times non-existent.

-- Q. Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this authority (legislation, mandates, etc.
-- A. The DNM computerized database contains the list of INTERPOL fugitives and Uruguayan fugitives, but wanted persons are not denied entry to Uruguay. Instead, the Uruguay National Police INTERPOL Office is notified and the person is arrested.

-- Q. What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? Which agency would question, detain, or deny entry?
-- A. DNM is only permitted very limited questioning beyond checking the traveler,s documents. No one is denied entry to the country. If the traveler is a fugitive, the police detain the traveler.

-- Q. How well does information sharing function within the host government, e.g., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally?

-- A. The police are immediately notified and the police detain the person, but the traveler is never denied entry into Uruguay.

¶D. Biometric Collection

-- Q. Are biometric systems integrated for all active POEs? What are the systems and models used?

-- A. No.

-- Q. Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e-Passport) or one to many comparison (checking the biometric presented against a database of known biometrics)?

-- A. Not applicable.

-- Q. If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints?

-- A. Not applicable.

-- Q. What are the host government's policies on collecting the fingerprints of travelers coming into the country?

-- A. DNM is not authorized to collect fingerprints of travelers.

-- Q. Which agency is responsible for the host government's fingerprint system?

-- A. Policia Tecnica, Policia Nacional de Uruguay. Individual's seeking residence in Uruguay submit police clearances from each country they lived in for more than 6 months, and then INTERPOL then takes those fingerprints and forwards them to the FBI for clearance.

-- Q. Are the fingerprint programs in place NIST, INT-I, EFTS, UK1 or RTID compliant?

-- A. INT-I compliant

-- Q. Are the fingerprints collected as flats or rolled? Which agency collects the fingerprints?

-- A. Rolled, taken by la Policia Technica.

¶E. Passports

-- Q. If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments?

-- A. Machine-readable passports have been available for the past five years, but not all passports issued during that time are machine-readable. The consular section continues to see hand-written passports from overseas Uruguayan missions and official passports that are hand-written.

-- Q. Does the host government issue replacement passports for full or limited validity (e.g. the time remaining on the original passports, fixed validity for a replacement, etc.)?

-- A. Emergency replacement consular passports are only valid for eight days, one use and are surrendered upon return to Uruguay. A regular 5-year passport can be obtained at consulates, but requires all of the normal checks and IDs which take about three months when requested in a foreign country.

-- Q. Does the host government have special regulations/procedures for dealing with "habitual" losers of passports or bearers who have reported their passports stolen multiple times?

-- A. The Consular section is not aware of any special procedures. No other information is available.

-- Q. Are replacement passports of the same or different appearance and page length as regular passports (do they have something along the lines of our emergency partial duration passports)?

-- A. All passports issued in Uruguay are identical and machine-readable. Consular emergency passports issued outside of Uruguay are different in appearance and not machine-readable.

-- Q. Do emergency replacement passports contain the same or fewer biometric fields as regular-issue passports?

-- A. Not Applicable

-- Q. Where applicable, has Post noticed any increase in the number of replacement or "clean" (i.e. no evidence of prior travel) passports used to apply for U.S. visas?

-- A. No discernible increase in the use of 'clean' passports, but the number of applicants that try and use this tactic to disguise their travel is steady. When applicants are unable to provide past passports in order to provide proof of previous travel, the consular section (CONS) requests that they obtain an immigration report from DNM. In two cases, CONS found fraudulent immigration reports when they cross checked with DNM directly. The DNM employees involved were fired and prosecuted.

-- Q. Are replacement passports assigned a characteristic number series or otherwise identified?

-- A. All passports have the same number as the Uruguayan cedula. There is no identification or characteristic for replacement passports, nor even a annotation indicating that it is a replacement. This has created problems for the GOU at POEs, because the passport number in the replacement passport is the name as the old passport, which has been reported as missing.

¶F. Fraud Detection

-- Q. How robust is fraud detection and how actively are instances of fraud involving documents followed up?

-- A. Fake documents are reported to the police.

-- Q. How are potentially fraudulently issued documents taken out of circulation, or made harder to use?

-- A. Fake documents are given to the police.

¶G. Privacy and Data Security

-- Q. What are the country's policies on records related to the questioning, detention or removal of individuals encountered at points of entry into the country? How are those records stored, and for how long?

-- A. DNM records are maintained at DNM Headquarters, but again DNM questioning is very limited and no one is denied entry into the country.

-- Q. What are the country's restrictions on the collection or use of sensitive data?

-- A. Not authorized.

-- Q. What are the requirements to provide notice to the public on the implementation of new databases of records?

-- A. Any changes require new legislation. DNM has a webpage with general information for the traveling public.

-- Q. Are there any laws relating to security features for government computer systems that hold personally identifying

information?
-- A. No. Only DNM internal regulations and practices.

-- Q. What are the rules on an individual's ability to access data that homeland security agencies hold about them?
-- A. This information is confidential and not shared with the public. However, an individual is able to request and receive a record of their own entries and exits.

-- Q. Are there different rules for raw data (name, date of birth, etc.) versus case files (for example, records about enforcement actions)?
-- A. Post does not have any information on this question.

-- Q. Does a non-citizen/resident have the right to sue the government to obtain these types of data?
-- A. Post believes that a non-citizen/non-resident has the right to ask for their own record of entries and departures. Police clearance records are also available to an individual for clearance and immigration purposes.

¶H. Immigration Data Bases

-- Q. What computerized immigration databases are used to track entries and exits?
-- A. The DNM system is named Registro de Analysis de los Movimientos Migratorios (RAM).

-- Q. Is the immigration database available at all ports of entry (POEs)?
-- A. No, presently installed at Montevideo and Punta del Este airports, Montevideo and Colonia seaports, and the bridge at Fray Bentos. In six months RAM will be installed at all POEs.

-- Q. If immigration databases are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?
-- A. In six months RAM will be installed at all POEs.

-- Q. What problems, if any, limit the effectiveness of the systems? For example, limited training, power brownouts, budgetary restraints, corruption, etc.?
-- A. The RAM system has UPS to deal with power brownouts. No other problems were mentioned.

-- Q. How often are national immigration databases updated?
-- A. The RAM system is continually updated.

¶I. Watchlist and Information Sharing

-- Q. Is there a name-based watchlist system used to screen travelers at POEs?
-- A. No.

-- Q. What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, criminal wants/warrants?
-- A. DNII and criminal warrants, including interpol.

-- Q. What international watchlists does the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.?

SIPDIS
-- A. The DNM system is named Registro de Analysis de los Movimientos Migratorios (RAM) and includes INTERPOL fugitives.

-- Q. What bilateral/multilateral watchlist agreements exist between host government and its neighbors?
-- A. NONE.

¶J. Biometrics

-- Q. Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system?
-- A. No.

-- Q. If biometric systems are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?
-- A. Not Applicable.

-- Q. What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris recognition, hand geometry, retinal identification, DNA-based identification, keystroke dynamics, gait analysis? Are the systems ICAO compliant?
-- A. Not Applicable.

-- Q. Does the host government issue a machine-readable passport containing biometric information? If e-Passports are issued, what biometric information is included on the document i.e. fingerprint, iris, facial recognition, etc? If not, does host government plan to issue a biometric document in the future? When?
-- A. Not Applicable. No plans at present to issue biometric documents.

Identifying Appropriate Partners

-- Q. Department would appreciate post's assessment of whether host government would be an appropriate partner in data sharing.
-- A. New legislation would be needed before a data sharing agreement could be entered into with the Uruguayan government.

-- Q. Considerations include whether host government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc.
-- A. Not Applicable.

-- Q. Are there political realities which would preclude a country from entering into a formal data-sharing agreement with the U.S?

-- A. The left-leaning Frente Amplio government has been reluctant to public acknowledge current and potential security cooperation with the USG. Privately, the GOU has been very cooperative with both the RSO and other agencies at post. The DNII routinely shares data with the RSO, including biographical information, wants/warrants, police records, financial information, vehicle registrations/address, radical affiliations, and other information (close hold this information).
-- Q. Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information?
-- A. Yes.

-- Q. How much information sharing does the host country do internally? Is there a single consolidated database, for example? If not, do different ministries share information amongst themselves?
-- A. DNM shares information with the police, but there is no consolidated database and the RAM system is only accessible to DNM personnel.

-- Q. How does the country define terrorism? Are there legal statutes that do so?
-- A. Uruguay is a party to all thirteen United Nations conventions combating international terrorism. Uruguayan Public laws 14.728, 17.835 and 18.070 address issues of

terrorism. Uruguay is also party to the Inter-American
Convention Against Terrorism.

End Report.

¶3. (C) Comment. Embassy has identified and will report on several possible ways for the GOU to improve its information collection, screening and sharing activities, including computer/database needs. End Comment.
Harding